(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 05 487 A 1**

(51) Int. Cl.[7]:
G 07 C 9/00
H 04 L 9/32

(21) Aktenzeichen: 100 05 487.0
(22) Anmeldetag: 8. 2. 2000
(43) Offenlegungstag: 9. 8. 2001

DE 100 05 487 A 1

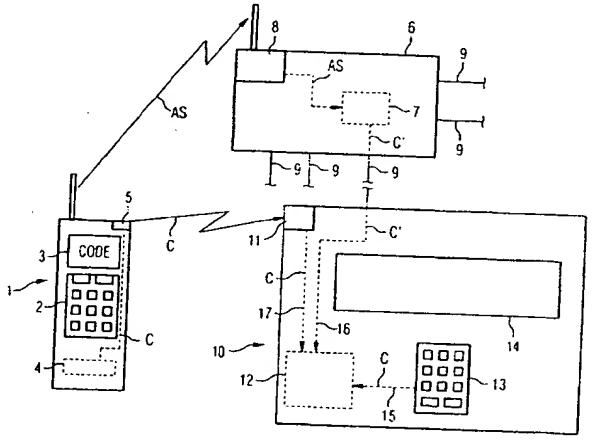
(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Prange, Stefan, Dr.-Ing., 81476 München, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zur Nutzeridentitätskontrolle

(57) Beschrieben wird ein Verfahren zur Nutzeridentitätskontrolle an einem Dienstterminal. Hierbei wird unter Verwendung eines Endgeräts des Nutzers und/oder ansprechend auf ein Anforderungssignal des Endgeräts ein Code für das Endgerät generiert und dieser Code vom Endgerät zur Entschlüsselung und/oder Verifizierung an das Dienstterminal übermittelt.



DE 100 05 487 A 1

für einen Nutzungsvorgang ein bestimmter Code ausgewählt wird. Auch bei dieser Ausführungsform wäre schon eine relativ große Sicherheit gegeben, wenn der Bestand an Codes groß genug gewählt wird.

Vorzugsweise ist der Code jedoch ein eindeutig dem jeweiligen Nutzungsvorgang zugeordneter Code, welcher speziell für den Nutzungsvorgang generiert und nur einmal verwendet wird.

Bei einer besonders vorteilhaften Ausführungsform wird der Code unter Verwendung eines dem Nutzungsvorgang und/oder dem Diensteterminal zugeordneten Parameters generiert. Ein solcher Parameter ist beispielsweise das Datum, die Uhrzeit, bei einem Bezahlvorgang der Betrag, der Ort der Nutzung, z. B. der Name oder eine Kennummer eines Geschäftes, oder eine Nummer des Diensteterminals. Diese Parameter können, wie beispielsweise das Datum oder die Uhrzeit, automatisch durch eine im Endgerät befindliche Uhr generiert werden. Andere Parameter wie Betrag oder Terminalnummer können beispielsweise auch von Hand durch den Benutzer in das Endgerät eingegeben werden. Der Ort läßt sich beispielsweise durch eine Lokalisierungseinrichtung des Geräts, wie z. B. durch ein auf GPS oder einem Funknetz basierenden Ortungssystem, auch automatisch feststellen.

Bei einer weiteren vorteilhaften Ausführungsform wird der Code unter Verwendung eines eindeutig dem Nutzer bzw. dem Endgerät zugeordneten Parameters generiert. Hierbei kann es sich um eine Kundenidentitätsnummer, eine Telefonnummer oder eine Kreditkartennummer des Nutzers handeln. Insbesondere kann es sich hierbei auch um eine PIN handeln, das heißt, es wird nur dann ein Zugangscode ausgegeben, wenn die richtige PIN eingegeben wird. In diesem Fall wäre die gleiche Sicherheit gegeben wie bei der Benutzung von Kreditkarten mit einer PIN, die am Diensteterminal eingegeben wird. Jedoch hat dieses Verfahren den Vorteil, daß sich der Benutzer nur eine PIN merken muß und mit dieser PIN die verschiedensten Zugangscodes für die unterschiedlichsten Dienste bzw. Diensteterminals erzeugen kann.

Für hohe Sicherheitsstufen können als Parameter auch biometrische Daten des Nutzers, beispielsweise ein Fingerabdruckmuster oder dergleichen, verwendet werden. Hierzu muß das Endgerät lediglich eine entsprechende Einrichtung zum Einlesen der biometrischen Daten aufweisen. Bei der Codegenerierung können die genannten Parameter entweder direkt als Ausgangsparameter verwendet werden, aus denen der Code generiert wird. Es ist aber auch möglich, daß die Parameter nicht direkt in den Code selbst eingehen, sondern lediglich insoweit verwendet werden, als daß ihre Richtigkeit geprüft wird und erst dann ein Code generiert wird. Es ist selbstverständlich auch eine beliebige Kombination der verschiedenen Parameter möglich.

Die Generierung des Codes für das Endgerät kann z. B. im Endgerät selbst in einer entsprechenden Codegenerierungseinrichtung erfolgen. Diese interne Codegenerierungseinrichtung kann sich aber auch auf einer SIM-Karte o. ä. auswechselbarem Modul im Endgerät befinden.

Die Codegenerierung kann jedoch auch in einer externen Codegenerierungseinrichtung, beispielsweise eines zentralen Anbieters im Netz, erfolgen. Es ist auch eine teilweise Generierung des Codes in einer zentralen Einrichtung im Netz und im Gerät bzw. auf einer SIM-Karte oder dergleichen möglich. Das heißt, der Algorithmus zur Erzeugung des Codes befindet sich teilweise im Endgerät und teilweise im Netz. Hierdurch sind beliebig hohe Sicherheitsstufen erreichbar.

Die Erzeugung des Codes in einer externen Codegenerierungseinrichtung erfolgt vorzugsweise durch ein Anforderungssignal, welches vom Endgerät an die Codegenerierungseinrichtung gesendet wird. Dies kann beispielsweise bei einem Mobiltelefon über SMS erfolgen. Dieses Anforderungssignal kann u. a. die genannten dem Diensteterminal, dem Nutzungsvorgang, dem Nutzer oder dem Endgerät zugeordneten Parameter enthalten.

Ebenso kann für das Diensteterminal ein Code erzeugt werden, der dazu benutzt wird, den Code des Endgeräts zu entschlüsseln oder in anderer geeigneter Weise zu verifizieren. Eine einfache Möglichkeit besteht darin, daß beide Codes identisch sind und ein Vergleich der Codes stattfindet. Nur bei Übereinstimmung der Codes wird dann die Transaktion durchgeführt.

Vorzugsweise wird der Code jedoch mit einem asymmetrischen Verschlüsselungsverfahren erzeugt. Das heißt, der Schlüssel des Endgeräts zum Erzeugen des Codes und der Schlüssel des Diensteterminals, um den Code zu entschlüsseln oder zu verifizieren und den Nutzer bzw. das Endgerät zu identifizieren, sind unterschiedlich.

Der Code kann dabei von einer im Diensteterminal befindlichen Codegenerierungseinrichtung oder einer externen Codegenerierungseinrichtung, beispielsweise einer Codegenerierungseinrichtung in einem Netz von mehreren Diensteterminals, generiert werden. Es kann sich hierbei insbesondere auch um die gleiche Codegenerierungseinrichtung handeln, die auch den Code für das Endgerät erzeugt. In diesem Fall würde aufgrund des Anforderungssignals in der Codegenerierungseinrichtung ein Code erzeugt und an das Endgerät und an das Diensteterminal versendet.

Bei einem weiteren bevorzugten Ausführungsbeispiel werden die Codes separat, d. h. der Code für das Endgerät des Nutzers vom Endgerät selbst und der Code für das Diensteterminal von der internen oder externen Codegenerierungseinrichtung generiert. In diesem Fall kann beispielsweise gleichzeitig mit der Generierung des Codes im Endgerät ein entsprechendes Anforderungssignal an die Codegenerierungseinrichtung erfolgen, woraufhin der Code für das Diensteterminal erzeugt wird.

Bei einer weiteren bevorzugten Ausführungsform wird der Code für das Endgerät oder der Code für das Diensteterminal bzw. beide Codes jeweils in einem rekursiven Verfahren unter Verwendung des bei dem vorherigen Nutzungsvorgang verwendeten Codes generiert. Bei dem rekursiven Verfahren handelt es sich vorzugsweise um einen geheimen Algorithmus, um einen möglichst hohen Sicherheitsstandard zu erreichen. Es ist auch möglich, daß der Code nur teilweise unter Verwendung eines rekursiven Verfahrens erzeugt wird. Das heißt, es wird quasi ein Grundcode rekursiv erzeugt und zur Erzeugung des endgültigen Zugangscodes werden dann weitere Parameter, beispielsweise die dem Nutzungsvorgang zugeordneten Parameter wie Datum, Uhrzeit, Betrag, Ort oder die dem Endgerät bzw. dem Nutzer zugeordneten Parameter wie PIN, hinzugefügt und daraus der Gesamtcode generiert.

Bei einem rekursiven Verfahren zur Erzeugung des Codes für das Diensteterminal und einer separaten Erzeugung des Codes für das Endgerät kann das Anforderungssignal zur Erzeugung eines Codes für das Diensteterminal auch implizit mit der Übersendung des Codes an das Diensteterminal bei dem vorherigen Nutzungsvorgang erfolgen. Das heißt, bei Übersendung des Codes bei einem Nutzungsvorgang wird automatisch gleich vom Diensteterminal bzw. von der externen Codegenerierungseinrichtung des Diensteterminals ein neuer Code für den nächsten Nutzungsvorgang erzeugt und in einem Speicher abgelegt.

Ein erfindungsgemäßes Endgerät weist je nach Art des erfindungsgemäßen Verfahrens entweder eine interne Codegenerierungseinrichtung oder eine entsprechende Einrichtung

Gleichzeitig wird ein Anforderungssignal AS über einen SMS-Kanal des Mobilfunknetzes direkt an die Empfangseinrichtung **8** des zentralen Rechners **6** übermittelt. Dieses Anforderungssignal AS wird an die Codegenerierungseinrichtung **7** weitergeleitet. Das Anforderungssignal AS enthält u. a. die von der Codegenerierungseinrichtung **4** des Mobiltelefons **1** für die Generierung des Codes genutzten Daten. In der Codegenerierungseinrichtung **7** wird daraufhin parallel ein Code C' erzeugt, welcher an das Dienstesterminal **10** übermittelt wird. Über die Datenleitung **9**, **16** gelangt dieser Code C' zur Einrichtung **12** zur Verifizierung des vom Mobiltelefon **1** erzeugten Codes C.

Zur Übermittlung des Codes C von dem Mobiltelefon **1** zum Diensteterminal **10** bestehen verschiedene Möglichkeiten.

Zum einen kann eine direkte Übermittlung über die drahtlosen Funkschnittstellen **5**, **11** erfolgen. Weiterhin ist es möglich, daß der Code C in alphanumerischer Form auf dem Display **3** des Mobiltelefons **1** dargestellt wird. Dieser Code C kann dann vom Nutzer oder einer das Diensteterminal **10** bedienenden Person über die Tastatur **13** in das Diensteterminal **10** eingegeben werden.

Je nach Eingabeart gelangt der Code C über die Leitungen **15** oder **17** zur Einrichtung **12** zur Verifizierung des Codes C'. Hier wird der Code C entweder mit Hilfe des Codes C' entschlüsselt und so verifiziert oder bei Erzeugung eines identischen Codes C, C' für das Mobiltelefon **1** und das Diensteterminal **10** einfach verglichen. Das Diensteterminal **10** kann zusätzlich aufgrund des eingegebenen Codes C als Quittungscode eine Rechnung erzeugen, die dann noch vom Kunden, wie bei den bisherigen Zahlungsmethoden mit einer EC-Karte, unterschrieben wird.

Die **Fig. 2** und 3 zeigen eine alternative Methode zur Übergabe des Codes C. Hierbei wird auf dem Display **3** des Mobiltelefons **1** ein Codemuster, im vorliegenden Beispiel ein Muster, bestehend aus einem Balkencode C und einem darunter angeordneten alphanumerischen Code, erzeugt. Dieser Balkencode C wird dann über eine Leseeinrichtung **18** gelesen, indem das Mobiltelefon **1** mit dem Display **3** auf ein Scannerfenster **19** der Leseeinrichtung **18** des Diensteterminals **10** aufgelegt wird.

Die Leseeinrichtung **18** kann hierbei in das Diensteterminal **10** integriert sein. Es kann sich aber auch, wie dargestellt, um eine externe Leseeinrichtung **18** handeln, die durch eine entsprechende Leitung oder über eine drahtlose Verbindung mit dem Diensteterminal **10** kommuniziert. Im einfachsten Fall handelt es sich bei der Leseeinrichtung **18** beispielsweise um einen Laserscanner, welcher sich ohnehin am Diensteterminal **10** befindet, um Balkencodes auf Waren oder dergleichen einzulesen.

Wie die Beispiele zeigen, ist das erfindungsgemäße Verfahren äußerst universell und mit heute verfügbaren Endgeräten und Diensteterminals realisierbar, ohne daß aufwendige technische Änderungen oder neue Komponenten hinzugefügt werden müssen. Es sind lediglich Änderungen in den Steuerungen der jeweiligen Geräte erforderlich, wobei die verschiedenen Applikationen, beispielsweise bei Mobiltelefonen oder ähnlichen Geräten, auch auf entsprechenden SIM-Karten oder in anderen Modulen realisiert werden können.

Je nach Aufwand sind die verschiedensten Sicherheitsstufen erreichbar, indem zur Erzeugung des Codes verschiedene Parameter verwendet werden, welche eindeutig mit der Person des Nutzers oder mit dem Diensteterminal zusammenhängen. Weiterhin können beispielsweise über SMS vom Diensteterminal oder vom jeweiligen Endgerät zur Erhöhung der Sicherheit zusätzliche Nummern übermittelt werden, welche ebenfalls in die Generierung der Codes, d. h. zur Verschlüsselung bzw. auch zur Entschlüsselung, einfließen.

Die Algorithmen zur Erzeugung der Codes können beliebig kompliziert sein und können auf verschiedene Einrichtungen verteilt sein, so daß auch auf diese Weise die Sicherheit erhöht werden kann.

Da der Code für jede Transaktion nur einmal genutzt wird, muß hierbei an der kritischsten Stelle, nämlich bei der Übermittlung des Codes vom Endgerät an das Diensteterminal, welche in der Regel in der Anwesenheit von weiteren Personen, wie dem Bedienpersonal des Diensteterminals oder anderen Kunden, stattfindet, der Code nicht besonders geschützt werden.

Das Verfahren ersetzt somit auch aufwendige TAN-Listen und eignet sich insbesondere auch gut für die Bezahlung von Waren und Dienstleistungen per Internet. In diesem Fall wäre dann das Diensteterminal beispielsweise der eigene Computer des Nutzers. Die Codegenerierungseinrichtung befindet sich dabei beispielsweise in einem Server des Dienstanbieters. Zur Durchführung einer Transaktion mit dem Diensteterminal, beispielsweise beim Homebanking, kann der Nutzer wie bisher seine private Zugangsnummer nutzen und zusätzlich für jede Transaktion eine über das Endgerät erzeugte und ausgegebene Zugangsnummer verwenden, welche einmalig für die jeweilige Transaktion herausgegeben wird und damit die bisherige TAN ersetzt.

Patentansprüche

1. Verfahren zur Nutzeridentitätskontrolle an einem Diensteterminal (**10**), bei dem unter Verwendung eines Endgeräts (**1**) des Nutzers und/oder ansprechend auf ein Anforderungssignal (AS) des Endgeräts (**1**) ein Code (C) für das Endgerät (**1**) generiert und dieser Code (C) vom Endgerät (**1**) zur Entschlüsselung und/oder Verifizierung an das Diensteterminal (**10**) übermittelt wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Code (C) ein eindeutig dem jeweiligen Nutzungsvorgang zugeordneter Code (C) ist.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß für das Diensteterminal (**10**) ein Code (C') generiert wird und das Diensteterminal (**10**) unter Verwendung dieses Codes (C') den vom Endgerät (1) empfangenen Code (C) entschlüsselt und/oder verifiziert.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß vom Endgerät (**1**) des Nutzers ein Anforderungssignal (AS) an eine Codegenerierungseinrichtung (**7**) gesendet wird und daraufhin von der Codegenerierungseinrichtung (7) der Code (C') generiert und an das Diensteterminal (**10**) übermittelt wird.
5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß der von der Codegenerierungseinrichtung generierte Code als Code für das Endgerät an das Endgerät übermittelt wird.
6. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß die Codes (C, C') separat von dem Endgerät (**1**) des Nutzers und der Codegenerierungseinrichtung (**7**) generiert werden.
7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß der Code (C, C') jeweils ganz oder teilweise in einem rekursiven Verfahren unter Verwendung des bei dem vorherigen Nutzungsvorgangs verwendeten Codes generiert wird.
8. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Code (C, C') unter

Nummer: DE 100 05 487 A1
Int. Cl.[7]: G 07 C 9/00
Offenlegungstag: 9. August 2001

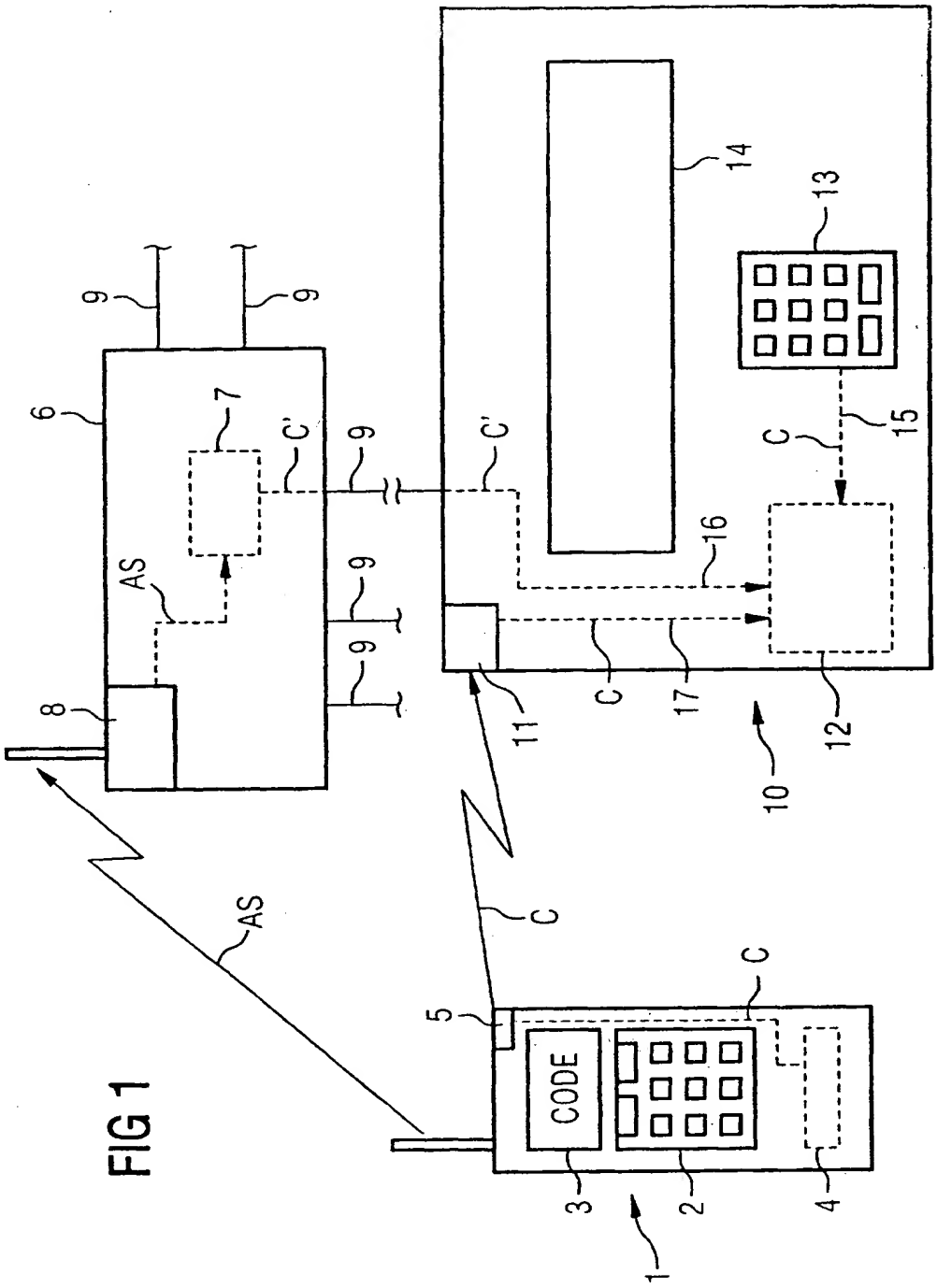


FIG 1